NIAC Working Group on Internet Hardening

Interim Progress Report

George Conrades, Chairman and CEO - Akamai Technologies

Presented by

Andy Ellis, Director of Information Security - Akamai Technologies

13 April 2004

Agenda

- Background
- Methodology
- Key Issues and Preliminary Considerations
- Next Steps

Background

- July 2003 meeting, President Bush asks NIAC what can be done to harden the Internet
- NIAC establishes a working group to address the challenge of Internet Hardening

Mission/Objectives

- Develop guidance based on best practices in Internet systems management
  - Infrastructure advice aimed at network operators
  - Customer environment advice aimed at end users and enterprise networks
- Evaluate long term technologies to improve the environment
- Derive policy recommendations for President Bush based on developed guidance
  - Government internal policies to increase security on government networks
  - Policies to incentivize private sector security improvements

Methodology

- Created two study groups
  - Infrastructure protection
  - Customer environment
- Meeting weekly for duration of working group
  - Assessing state of "best practices" published by other organizations

Study Group Participants

- George Conrades, Akamai
- Bora Akyol, Cisco
- Pete Allor, ISS
- Al Berkeley, Community of Science
- Matt Bishop, UCDavis
- Vint Cerf, MCI
- Steve Crocker, ICANN
- John Clarke, DHS
- Richard Clarke, GoodHarbor Consulting
- Sean Convery, Cisco
- Andy Ellis, Akamai
- John Faherty, DHS
- Noam Freedman, Akamai
- Peg Grayson, V-One
- Barry Greene, Cisco
- Matt Korn, AOL
- Deb Miller, V-One
- Bob Mahoney, MIT
- Gerry Macdonald, AOL
- Paul Nicholas, EOP
- Mike Petry, MCI
- Jeff Schiller, MIT
- Howard Schmidt, eBay
- Marty Schulman, Juniper
- Paul Vixie, ISC
- Ken Watson, Cisco
- Nancy Wong, DHS
- Lee Zeichner, GMU

Overall Findings

- Best Practices
  - Best Practice recommendation are usually aimed at the small and medium size players
  - We need to understand *why* people don't implement best practice recommendations to change their behavior
  - Because best practices take a long time to be adopted, improving the existing "best" practice is a good place to impact the large players
- New Technologies
  - New technologies can present opportunities to improve existing methods of engaging in business
  - Investment in new systems is often a barrier to adoption.

Key Issues & Findings

- Infrastructure
  - Two types of attacks that present risk
    - Attacks against pieces of the infrastructure
    - Attacks using the infrastructure
  - Areas of investigation
    - BGP - the routing fabric of the Internet
    - DNS - The name server that supports human-readable names
    - DDoS - Distributed attacks using or directed at the infrastructure

Key Issues & Findings

- Three possible ways to secure the infrastructure:
  1. Secure individual network elements
     - Educate users: harden passwords, etc.
     - Implement processes to ensure secure initial/default installations
     - Run systems against security checkers
     - More secure "control planes"

Key Issues & Findings

  2. Prefix Filtering
     - Explore development of a routing registry to store "allowed routes"
       - Potentially use soBGP or sBGP as an alternative
     - Many operational and management issues need to be addressed prior to global implementation
  3. Packet Filtering
     - BCP38 in non-multi-homed environments
     - When filtering on source addresses, filter on allowed prefixes vs. announced prefixes

Key Issues & Findings

- Customer Environment
  - Non-enterprise end users
    - Represent a target-rich environment for attackers to collect assets to use in DDoS attacks
    - Best practices are oriented around individual participation and education.
    - Incentives: public education and awareness, financial incentives to encourage the acquisition of security tools

Key Issues & Findings

- Customer Environment
  - Enterprise users
    - Protection steps need to be taken by corporate and public entities, not individuals
    - Incentives
      - Negative: regulation of private sector companies
      - Neutral: Government buying requirements
      - Positive: Provide education to company boards and audit committees to better enable broad corporate oversight

Next Steps

- Develop guidance based on current recommendations and existing best practices
- Draft and review report for the NIAC